Assignment

Here is the data
https://docs.google.com/spreadsheets/d/1MTnRFZvwCDI1lnrKsQXau-zqcPzDpkg_wsnkP0wkcaA/edit?usp=sharing

Column Descriptions

1. Date Or Hour
The date and time (usually at the start of the hour or day) representing when the aggregated data was recorded.

2. unique_idfas
The number of unique device identifiers (IDFAs) seen in the traffic. This represents the count of unique devices generating ad requests.

3. unique_ips
The number of unique IP addresses from which the ad requests originated. This helps identify whether traffic is coming from diverse locations or concentrated networks.

4. unique_uas
The number of unique User-Agent strings detected. User-Agents identify the type of device or app sending requests. Too few or too many can indicate suspicious or inconsistent traffic.

5. total_requests
The total number of ad requests received during the given time period. It shows the overall volume of ad traffic from all devices.

6. requests_per_idfa
Calculated as `total_requests / unique_idfas`. This ratio indicates how many ad requests each device sent on average. Abnormally high or low ratios may suggest automated or replayed traffic.

7. impressions
The total number of ads successfully rendered or shown. Comparing this with requests helps assess delivery efficiency and potential fake or unserved requests.

8. impressions_per_idfa
Calculated as `impressions / unique_idfas`. This shows how many impressions each device received on average. Low or zero values suggest requests without real ad delivery.

9. idfa_ip_ratio
Calculated as `unique_idfas / unique_ips`. This measures how many unique devices are

seen per IP address. Normally close to 1 in real environments; a high value may suggest proxy or datacenter traffic.

10. idfa_ua_ratio
Calculated as `unique_idfas / unique_uas`. This shows how many devices share the same User-Agent. A very high ratio indicates possible device spoofing, where many fake devices pretend to have the same setup.

11. IVT
Stands for **Invalid Traffic** — a metric estimating the level of suspicious or non-human traffic. It is often derived from ratios like `idfa_ua_ratio` or other fraud detection signals. High values indicate likely bot or spoofed traffic.

We have 3 apps data which donot marked as ivt
And 3 apps which got marked IVT at different point of time

Now need to analyse why what pattern traffic has that some marked no ivt, some marked ivt earlier some later on.

Try to get analytics on this

Send details on manneajeet@huntdigitalmedia.com